• • •

RECURSO EM MANDADO DE SEGURANÇA Nº 61.302 / RIO DE JANEIRO (2019/0199132-0)

RELATOR: MINISTRO ROGERIO SCHIETTI CRUZ
RECORRENTE: GOOGLE BRASIL INTERNET LTDA.
RECORRENTE: GOOGLE LLC
ADVOGADOS: EDUARDO BASTOS FURTADO DE MENDONÇA - RJ130532
FELIPE MENDONÇA TERRA - RJ179757
NAIANA DO AMARAL PORTO - RJ167818
JACQUELINE DE SOUZA ABREU - SP356941
RECORRIDO: MINISTÉRIO PÚBLICO DO ESTADO DO RIO DE JANEIRO
INTERES.: FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA.
ADVOGADOS: CARLOS ANTÔNIO PENA - SP105802
ANTÔNIO SÉRGIO ALTIERI DE MORAES PITOMBO - SP124516
GUILHERME ALFREDO DE MORAES NOSTRE - SP130665
CLAUDIO MAURO HENRIQUE DAÓLIO - SP172723
FLÁVIA MORTARI LOTFI - SP246694
IZABEL DE ARAÚJO CORTEZ - SP235560
BEATRIZ DE OLIVEIRA FERRARO - SP285552
JULIA THOMAZ SANDRONI - RJ144384
LARA MAYARA DA CRUZ - SP305340
RAFAEL SILVEIRA GARCIA - DF048029
BIANCA DIAS SARDILLI - SP299813

EMENTA

RECURSO EM MANDADO DE SEGURANÇA. DIREITO À PRIVACIDADE E À INTIMIDADE. IDENTIFICAÇÃO DE USUÁRIOS EM DETERMINADA LOCALIZAÇÃO GEOGRÁFICA. IMPOSIÇÃO QUE NÃO INDICA PESSOA INDIVIDUALIZADA. AUSÊNCIA DE ILEGALIDADE OU DE VIOLAÇÃO DOS PRINCÍPIOS E GARANTIAS CONSTITUCIONAIS. FUNDAMENTAÇÃO DA MEDIDA. OCORRÊNCIA.

PROPORCIONALIDADE. RECURSO EM MANDADO DE SEGURANÇA NÃO PROVIDO.

1. Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionados às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. No Brasil, a Constituição Federal, no art. 5º, X, estabelece que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". A ideia de sigilo expressa verdadeiro direito da personalidade, notadamente porque se traduz em garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital.

2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública.

3. Na espécie, a ordem judicial direcionou-se a dados estáticos (registros), relacionados à identificação de usuários em determinada localização geográfica que, de alguma forma, possam ter algum ponto em comum com os fatos objeto de investigação por crimes de homicídio.

4. A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5º, X, da CF/88 garante

a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma.

5. Os dispositivos que se referem às interceptações das comunicações indicados pelos recorrentes não se ajustam ao caso *sub examine*. O procedimento de que trata o art. 2º da Lei nº 9.296/1996, cujas rotinas estão previstas na Resolução nº 59/2008 (com alterações ocorridas em 2016) do CNJ, os quais regulamentam o art. 5º, XII, da CF, não se aplicam a procedimento que visa a obter dados pessoais estáticos armazenados em seus servidores e sistemas informatizados de um provedor de serviços de internet. A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados.

6. Não há como pretender dar uma interpretação extensiva aos referidos dispositivos, de modo a abranger a requisição feita em primeiro grau, porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é devidamente prevista no Marco Civil da Internet, o qual não impõe, entre os requisitos para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios.

7. Os arts. 22 e 23 do Marco Civil da Internet, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios, o que, aliás, seria até, na espécie – se houvesse tal obrigatoriedade legal –, plenamente dedutível da complexidade e da dificuldade de identificação da autoria mediata dos crimes investigados.

8. Logo, a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outros dados pessoais e informações,

não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo precípuo dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado.

9. Conforme dispõe o art. 93, IX, da CF, "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação". Na espécie, tanto os indícios da prática do crime, como a justificativa quanto à utilização da medida e o período ao qual se referem os registros foram minimamente explicitados pelo Magistrado de primeiro grau.

10. Quanto à proporcionalidade da quebra de dados informáticos, ela é adequada, na medida em que serve como mais um instrumento que pode auxiliar na elucidação dos delitos, cuja investigação se arrasta por dois anos, sem que haja uma conclusão definitiva; é necessária, diante da complexidade do caso e da não evidência de outros meios não gravosos para se alcançarem os legítimos fins investigativos; e, por fim, é proporcional em sentido estrito, porque a restrição a direitos fundamentais que dela redundam – tendo como finalidade a apuração de crimes dolosos contra a vida, de repercussão internacional – não enseja gravame às pessoas eventualmente afetadas, as quais não terão seu sigilo de dados registrais publicizados, os quais, se não constatada sua conexão com o fato investigado, serão descartados.

11. Logo, a ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, porquanto, tendo como norte a apuração de gravíssimos crimes cometidos por agentes públicos contra as vidas de três pessoas – mormente a de quem era alvo da emboscada, pessoa dedicada, em sua atividade parlamentar, à defesa dos direitos de minorias que sofrem com a ação desse segmento podre da estrutura policial fluminense – não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos pela diligência questionada.

12. Recurso em mandado de segurança não provido.

ACÓRDÃO

Vistos e relatados estes autos em que são partes as acima indicadas, acordam os Ministros da Terceira Seção, por maioria, negar provimento ao recurso em mandado de segurança, nos termos do voto do Sr. Ministro Relator. Vencido o Sr. Ministro Sebastião Reis Júnior que dava provimento ao recurso. Os Srs. Ministros Reynaldo Soares da Fonseca, Ribeiro Dantas, Antonio Saldanha Palheiro, Joel Ilan Paciornik, Felix Fischer, Laurita Vaz e Jorge Mussi votaram com o Sr. Ministro Relator.

Votou vencido o Sr. Ministro Sebastião Reis Júnior.

Presidiu o julgamento o Sr. Ministro Nefi Cordeiro.

O Dr. Eduardo Bastos Furtado de Mendonça sustentou oralmente pelas partes recorrentes: Google Brasil Internet Ltda. e Google LLC.

O Dr. Orlando Carlos Neves Belém, Procurador de Justiça, sustentou oralmente pela parte interessada: Ministério Público do Estado do Rio de Janeiro.

Brasília, 26 de agosto de 2020.

MINISTRO ROGERIO SCHIETTI CRUZ

RECURSO EM MANDADO DE SEGURANÇA Nº 61.302 / RIO DE JANEIRO (2019/0199132-0)

RELATOR: MINISTRO ROGERIO SCHIETTI CRUZ

RECORRENTE: GOOGLE BRASIL INTERNET LTDA.

RECORRENTE: GOOGLE LLC

ADVOGADOS: EDUARDO BASTOS FURTADO DE MENDONÇA - RJ130532
FELIPE MENDONÇA TERRA - RJ179757
NAIANA DO AMARAL PORTO - RJ167818
JACQUELINE DE SOUZA ABREU - SP356941

RECORRIDO: MINISTÉRIO PÚBLICO DO ESTADO DO RIO DE JANEIRO

INTERES.: FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA.

ADVOGADOS: CARLOS ANTÔNIO PENA - SP105802
ANTÔNIO SÉRGIO ALTIERI DE MORAES PITOMBO - SP124516
GUILHERME ALFREDO DE MORAES NOSTRE - SP130665
CLAUDIO MAURO HENRIQUE DAÓLIO - SP172723
FLÁVIA MORTARI LOTFI - SP246694
IZABEL DE ARAÚJO CORTEZ - SP235560
BEATRIZ DE OLIVEIRA FERRARO - SP285552

JULIA THOMAZ SANDRONI - RJ144384
LARA MAYARA DA CRUZ - SP305340
RAFAEL SILVEIRA GARCIA - DF048029
BIANCA DIAS SARDILLI - SP299813

RELATÓRIO

O SENHOR MINISTRO ROGERIO SCHIETTI CRUZ:

GOOGLE BRASIL INTERNET LTDA. e GOOGLE LLC interpõem recurso em mandado de segurança contra acórdão proferido pelo *Tribunal de Justiça do Estado do Rio de Janeiro*, que denegou a ordem impetrada naquela Corte, na qual questionavam a decisão do Juízo da 4ª Vara Criminal da Comarca do Rio de Janeiro, que *autorizou a identificação dos usuários de aplicativos de um conjunto não identificado de pessoas, tão somente pela circunstância aleatória de haverem transitado, em certo lapso de tempo, por determinadas coordenadas geográficas no Município do Rio de Janeiro - RJ (Ofícios nº 4.041/2018 e 4.047/2018)*.

Em suas razões, alegam os insurgentes, preliminarmente, que a determinação judicial ora impugnada perdeu o objeto, "tendo em vista a evolução da investigação e a identificação dos suspeitos dos crimes – inclusive por meio de outras provas e elementos fornecidos pela Google após decisões judiciais de quebra de sigilo" (fl. 144).

No mérito, afirmam que "a ordem jurídica brasileira não admite quebras de sigilo e interceptações genéricas, desprovidas de individualização razoável dos indivíduos afetados e das respectivas fundamentações" (fl. 154). No particular, assinalam que a premissa para quebras de sigilo, no sistema jurídico brasileiro, é a existência e demonstração de indícios concretos de envolvimento de determinada pessoa na prática de crimes e que não há previsão legal para quebra de sigilo com base em meras coordenadas geográficas.

Assinalam que "as localizações geográficas indicadas pela autoridade coatora criam o risco concreto de se afetar um número muito elevado de pessoas inocentes, já que abrangem extensas áreas do Rio de Janeiro – os polígonos englobam residências, repartições públicas, cartórios, escritórios de advocacia, hospitais, sindicatos, bancos, igrejas, escolas, hotéis, lojas, avenidas e pontos turísticos – e parte considerável deles sequer diz respeito à data e local do crime" (fl. 154).

Apontam a existência de conjunto normativo (arts. 5º, X, XII e 93, X, da Constituição Federal; 2º da Lei nº 9.296/1996; 22 do Marco Civil da Internet; 11 do Decreto-Federal nº 8.771/2016 e a Resolução CNJ nº 59/2008) que é suficiente para constatar que a quebra do sigilo é medida excepcional e, por isso mesmo, só poderia ser justificada pela existência de indícios concretos de atividade ilícita por parte do alvo delimitado, a serem demonstrados em decisão judicial fundamentada.

Sustentam que "as ordens aqui questionadas, contudo, não possuem esse tipo de limitação. Pelo contrário, chegam a alcançar milhares de cidadãos inocentes que

tenham estado, em horários comerciais, em amplas áreas urbanas da cidade do Rio de Janeiro – daí, portanto, a evidente violação à legislação regente" (fl. 170).

Por fim, aduzem que houve a inobservância ao princípio da proporcionalidade, porquanto a quebra de sigilo pretendida é *inadequada*, ao não oferecer mínima garantia de que levará ao autor ou aos autores dos delitos investigados, e que não há garantia de confiabilidade nos dados de geolocalização a serem pesquisados; é *desnecessária*, uma vez que há medidas e diligências alternativas que podem ser e foram tomadas pelas autoridades policiais; e *desproporcional* em sentido estrito, pois a determinação aceita o dano colateral de quebrar o sigilo de inocentes, assumindo que a medida extrema seria justificável pela possibilidade, apenas eventual, de se obter alguma pista sobre aqueles que teriam envolvimento nos crimes investigados.

O *Ministério Público do Estado do Rio de Janeiro*, em contrarrazões, às fls. 198-203, pronunciou-se acerca do recurso interposto, nestes termos, no que interessa (fls. 201-202):

> Não obstante a relevância da previsão do artigo 5° da Carta constitucional, a inteligência da hermenêutica revela que os direitos fundamentais não são absolutos, de modo que serão ponderados e/ou flexibilizados diante de outros direitos e interesses de igual ou semelhante importância.
>
> Nesse sentido, a própria redação do inciso XII do artigo 5° da Constituição da República, ao prever a possibilidade do afastamento e/ou relativização do direito ao sigilo de dados, por meio de ordem judicial, para fins de investigação criminal ou instrução processual penal, hipótese plenamente adequada ao caso em análise.
>
> A ponderação de interesses e direitos afigura-se especialmente imperiosa diante da relevância e complexidade da investigação criminal que deu causa à quebra de sigilo, cujo objeto é o assassinato da vereadora Marielle Franco e de seu motorista, Anderson Gomes, caso de notória repercussão social.
>
> Infere-se dos autos que a cautelar deferida se prestou identificação de usuários, e não ao acesso a teor dos dados de comunicação constantes de seus aparelhos telefônicos, o que, por si só, afasta a pretensa violação inconstitucional de sigilo.
>
> Pela mesma razão, destaque-se a improcedência de suposta violação ao princípio da presunção de inocência e ao devido processo legal, uma vez que a quebra de sigilo não pretendeu acesso aos dados usuários, afastando, assim, o argumento persecutório sustentado pelos recorrentes.

> Cumpre sublinhar, ainda, que a decisão ora impugnada visou a dar continuidade a minucioso trabalho investigativo, do qual já resultou a identificação de dois réus exatamente através da quebra de sigilo de dados.
>
> No que toca à suposta afronta aos ditames da Lei nº 12.965/2014 (Marco Civil da Internet), mister elucidar que a própria legislação, em seu artigo 3°, prevê a possibilidade da ponderação e/ou afastamento da proteção do direito à privacidade diante de direitos e interesses de igual relevância, sublinhando a coexistência dos princípios que anuncia com outras normas previstas no ordenamento jurídico brasileiro ou em tratados internacionais do qual a República faça parte.
>
> Noutro giro, a respeito do pleito apresentado pelas pessoas jurídicas recorrentes, mister trazer à baila o entendimento desse tribunal superior, ao decidir não ser cabível a impetração de mandado de segurança com vistas a se imiscuir em investigação que sequer recai sobre os impetrantes.

Ouvido, o Ministério Público Federal, em parecer subscrito pelo Subprocurador-Geral da República Marcelo Muscogliati, manifestou-se pelo provimento do recurso "para conceder a segurança rogada na impetração originária, qual seja, qual seja, cassar o mandado judicial de quebra de sigilo telemático circunscrito aos Ofícios nº 4041 e 4047 de 2018" (fl. 320).

Em 10/8/2020, as recorrentes apresentaram parecer jurídico, às fls. 364-408, produzido pelo Prof. Gilson Dipp, no qual, além de reiterar os argumentos externados neste recurso em mandado de segurança, assinalou que "medidas dessa natureza – quebras de sigilo genéricas, com base em coordenadas geográficas – têm sido reiteradamente cassadas pela ampla maioria das decisões dos Eg. Tribunais de Justiça'. O ponto foi também corroborado pelo Ministério Público Federal (fl. 364).

RECURSO EM MANDADO DE SEGURANÇA Nº 61.302 / RIO DE JANEIRO (2019/0199132-0)

EMENTA

> RECURSO EM MANDADO DE SEGURANÇA. DIREITO À PRIVACIDADE E À INTIMIDADE. IDENTIFICAÇÃO DE USUÁRIOS EM DETERMINADA LOCALIZAÇÃO GEOGRÁFICA. IMPOSIÇÃO QUE NÃO INDICA PESSOA INDIVIDUALIZADA. AUSÊNCIA DE ILEGALIDADE OU DE VIOLAÇÃO DOS PRINCÍPIOS E GARANTIAS CONSTITUCIONAIS. FUNDAMENTAÇÃO DA MEDIDA. OCORRÊNCIA. PROPORCIONALIDADE. RECURSO EM MANDADO DE SEGURANÇA NÃO PROVIDO.

1. Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionados às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. No Brasil, a Constituição Federal, no art. 5º, X, estabelece que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". A ideia de sigilo expressa verdadeiro direito da personalidade, notadamente porque se traduz em garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital.

2. Mesmo com tal característica, o direito ao sigilo não possui, na compreensão da jurisprudência pátria, dimensão absoluta. De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, assim como a Suprema Corte, entende que é possível afastar sua proteção quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública.

3. Na espécie, a ordem judicial direcionou-se a dados estáticos (registros), relacionados à identificação de usuários em determinada localização geográfica que, de alguma forma, possam ter algum ponto em comum com os fatos objeto de investigação por crimes de homicídio.

4. A determinação do Magistrado de primeiro grau, de quebra de dados informáticos estáticos, relativos a arquivos digitais de registros de conexão ou acesso a aplicações de internet e eventuais dados pessoais a eles vinculados, é absolutamente distinta daquela que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o seu destinatário. Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Decerto que o art. 5º, X, da CF/88 garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, o acesso a esses

dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma.

5. Os dispositivos que se referem às interceptações das comunicações indicados pelos recorrentes não se ajustam ao caso *sub examine*. O procedimento de que trata o art. 2º da Lei nº 9.296/1996, cujas rotinas estão previstas na Resolução nº 59/2008 (com alterações ocorridas em 2016) do CNJ, os quais regulamentam o art. 5º, XII, da CF, não se aplicam a procedimento que visa a obter dados pessoais estáticos armazenados em seus servidores e sistemas informatizados de um provedor de serviços de internet. A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados.

6. Não há como pretender dar uma interpretação extensiva aos referidos dispositivos, de modo a abranger a requisição feita em primeiro grau, porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é devidamente prevista no Marco Civil da Internet, o qual não impõe, entre os requisitos para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios.

7. Os arts. 22 e 23 do Marco Civil da Internet, que tratam especificamente do procedimento de que cuidam os autos, não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Assim, para que o magistrado possa requisitar dados pessoais armazenados por provedor de serviços de internet, mostra-se satisfatória a indicação dos seguintes elementos previstos na lei: a) indícios da ocorrência do ilícito; b) justificativa da utilidade da requisição; e c) período ao qual se referem os registros. Não é necessário, portanto, que o magistrado fundamente a requisição com indicação da pessoa alvo da investigação, tampouco que justifique a indispensabilidade da medida, ou seja, que a prova da infração não pode ser realizada por outros meios, o que, aliás, seria até, na espécie – se houvesse tal obrigatoriedade legal – plenamente dedutível da complexidade e da dificuldade de identificação da autoria mediata dos crimes investigados.

8. Logo, a quebra do sigilo de dados armazenados, de forma autônoma ou associada a outros dados pessoais e informações, não obriga a autoridade judiciária a indicar previamente as pessoas que estão sendo investigadas, até porque o objetivo

precípuo dessa medida, na expressiva maioria dos casos, é justamente de proporcionar a identificação do usuário do serviço ou do terminal utilizado.

9. Conforme dispõe o art. 93, IX, da CF, "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação". Na espécie, tanto os indícios da prática do crime, como a justificativa quanto à utilização da medida e o período ao qual se referem os registros foram minimamente explicitados pelo Magistrado de primeiro grau.

10. Quanto à proporcionalidade da quebra de dados informáticos, ela é adequada, na medida em que serve como mais um instrumento que pode auxiliar na elucidação dos delitos, cuja investigação se arrasta por dois anos, sem que haja uma conclusão definitiva; é necessária, diante da complexidade do caso e da não evidência de outros meios não gravosos para se alcançarem os legítimos fins investigativos; e, por fim, é proporcional em sentido estrito, porque a restrição a direitos fundamentais que dela redundam – tendo como finalidade a apuração de crimes dolosos contra a vida, de repercussão internacional – não enseja gravame às pessoas eventualmente afetadas, as quais não terão seu sigilo de dados registrais publicizados, os quais, se não constatada sua conexão com o fato investigado, serão descartados

11. Logo, a ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, porquanto, tendo como norte a apuração de gravíssimos crimes cometidos por agentes públicos contra as vidas de três pessoas – mormente a de quem era alvo da emboscada, pessoa dedicada, em sua atividade parlamentar, à defesa dos direitos de minorias que sofrem com a ação desse segmento podre da estrutura policial fluminense – não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos pela diligência questionada.

12. Recurso em mandado de segurança não provido.

VOTO

O SENHOR MINISTRO ROGERIO SCHIETTI CRUZ (Relator):

I. SÍNTESE DA CONTROVÉRSIA

Em *14/03/2018*, a então Vereadora Marielle Francisco da Silva (*Marielle Franco*) e *Anderson* Pedro Mathias Gomes foram vítimas de homicídio; no mesmo contexto, Fernanda Gonçalves Chaves, de homicídio tentado. Em razão disso, instaurou-se inquérito policial perante a Polícia Civil do Estado do Rio de Janeiro, do qual resultou ação penal (*Processo nº 0072026-61.2018.8.19.001*) contra os acusados *Ronnie Lessa e Élcio Vieira de Queiroz*.

Ao primeiro réu, *Ronnie Lessa*, foi imputada "a suposta prática dos crimes previstos nos artigos 121, §2°, incisos I (motivo torpe) e IV (duas vezes, emboscada e recurso que dificultou a defesa da vítima) do Código Penal, em relação à vítima Marielle; 121, §2°, incisos IV (duas vezes, emboscada e recurso que dificultou a defesa da vítima) e V, em relação à vítima Anderson; 121, §2°, incisos IV (emboscada) e V, c/c artigo 14, inciso II, do Código Penal, em relação à vítima Fernanda e, por fim, artigo 180, todos na forma do art. 69, todos do Código Penal" (fl. 50).

Ao segundo denunciado, *Élcio Vieira Queiroz*, "foi imputada a suposta prática dos crimes previstos nos artigos 121, §2°, incisos I (motivo torpe) e IV (duas vezes, emboscada e recurso que dificultou a defesa da vítima) c/c art. 29, ambos do Código Penal, em relação à vítima Marielle; 121, §2°, incisos IV (duas vezes, emboscada e recurso que dificultou a defesa da vítima) e V, c/c art. 29, ambos do Código Penal em relação à vítima Anderson; 121, §2°, incisos IV (emboscada) e V, c/c artigo 14, inciso II, c/c art. 29, todos do Código Penal, em relação à vítima Fernanda, por fim, artigo 180, todos na forma do art. 69, todos do Código Penal." (fls. 50-51).

Entretanto, *ainda durante as investigações*, as quais acabaram por desencadear *diversas frentes investigatórias*, houve a seguinte determinação do Juízo da 4ª Vara Criminal do Estado do Rio de Janeiro, exarada em 23/11/2018 (fls. 56-60):

> a) Que o provedor de aplicação de internet GOOGLE INC., sob pena de incursão no crime de desobediência, além de multa diária no valor de R$100.000,00 (cem mil reais), até o limite de R$ 3.000.000,00 (três milhões de reais), em caso do descumprimento de determinação judicial, ou de seu cumprimento parcial, nos termos do art. 537 do NCPC, *forneça e disponibilize à Autoridade Policial e ao Ministério Público*, no prazo de 05 (cinco) dias, a contar do recebimento desta ordem, e usando-se de *parâmetro os polígonos e conjuntos formados e relacionados a seguir* [...] *na busca do levantamento destes usuários através das contas vinculadas aos dispositivos identificados e operando na área delimitada de cada conjunto de polígonos* com sistemas

> operacionais IOS, WINDOWS MOBILE, sistema de gerenciamento GOOGLE/ANDROID, pelo aplicativo GOOGLE MAPS ou pelo aplicativo WAZE [...].

Assim, o referido magistrado deferiu, como afirma a impugnação, "a quebra de sigilo telemático, de um conjunto não identificado de pessoas, unidas tão somente pela circunstância aleatória de terem transitado, em certo lapso de tempo, por *diversas coordenadas geográficas do Município do Rio de Janeiro/RJ (Ofício nº 4041/2018 e Ofício nº 4047/2018)*" (fl. 84).

Por isso, a questão versada nesta oportunidade é de *extrema relevância e complexidade*, não apenas porque envolve a discussão subjacente à apuração do assassinato da Vereadora Marielle Franco – com ampla repercussão, nacional e internacional, dado o contexto de possível eliminação de uma vida dedicada à proteção dos direitos de minorias e de combate a grupos estatais e paraestatais que oprimiam e oprimem, violentamente, moradores da periferia da cidade do Rio de Janeiro –, mas também porque traz a lume importante debate, amiúde veiculado em casos similares, *sobre o limite e o alcance das ordens judiciais de quebra de sigilo de dados informáticos*, quando circunscritas a determinada localização ou a períodos curtos de tempo, notadamente diante do aparente *confronto entre o direito à privacidade dos indivíduos em geral e o interesse público na atividade de persecução penal para a apuração e a responsabilização penal de autor(es) de gravíssimos crimes dolosos contra a vida, no contexto já assinalado*.

As recorrentes alegam que a recusa no fornecimento das informações requeridas nos *Ofícios nº 4.041/2018 e 4.047//2018* tem como causa a proteção do direito à privacidade dos seus usuários e, também, o fato de que a referida decisão *determina ordem para quebra do sigilo telemático de um conjunto não identificado de pessoas que teriam transitado, em determinado lapso de tempo, por algumas coordenadas geográficas do Município do Rio de Janeiro/RJ, situação esta que, em sua ótica, não encontra respaldo na legislação de regência, tampouco na Constituição Federal*.

Por isso, a afetação do tema para julgamento perante o colegiado da 3ª Seção do Superior Tribunal de Justiça. Tal procedimento é reforçado pelo recente julgamento, no âmbito desta Seção, do *Incidente de Deslocamento de Competência nº 24/RJ*, oportunidade em que ficou registrada a *relevância do fato*, uma vez que uma das vítimas seria vereadora e defensora dos direitos humanos, especialmente dos direitos das mulheres, bem como combatia, com sua atuação parlamentar, a violência policial e grupos paramilitares de atuação no Rio de Janeiro, compostos majoritariamente por policiais ou ex-policiais, e que contam, para seu agir desenvolto, com vínculos ao aparato oficial.

Centra-se a irresignação, portanto e resumidamente, *em três aspectos*: 1) ausência de base constitucional e legal para quebra de sigilo genérica e aleatória, sem a individualização dos alvos e imputação de infração penal, a ensejar a violação do devido processo legal, do princípio da presunção de inocência, da privacidade, do direito de

acesso à informação e da liberdade de comunicação; 2) ausência de fundamentação adequada da decisão que determinou a quebra do sigilo; 3) inobservância do princípio da proporcionalidade.

II. PRELIMINAR DE PERDA DO OBJETO

De início, afasto a afirmação das recorrentes quanto à possível perda de objeto da decisão que determinou a quebra do sigilo de dados. O interesse do Ministério Público na efetivação das medidas deferidas pelo Magistrado de primeiro grau ainda remanesce, sobretudo porque mesmo diante do oferecimento de denúncia contra dois acusados, *as investigações continuam em seus diversos desdobramentos, todos com a finalidade de apurar outros eventuais envolvidos na prática delituosa*.

Tal constatação evidencia-se pelo recente julgamento do *IDC nº 24*, de relatoria da Ministra *Laurita Vaz*, publicado no DJe 1º/7/2020, oportunidade em que ficou registrada a existência de recursos em mandado de segurança em tramitação nesta Corte, entre os quais o que ora se examina, cujo objeto é justamente a validade do acesso aos registros de dados relevantes para as investigações. Extraem-se, do acórdão, no particular, as seguintes passagens:

> EM TODOS OS CASOS, o que se verifica, de maneira nítida, é a oposição da GOOGLE BRASIL INTERNET LTDA., GOOGLE LLC e o FACEBOOK ao fornecimento de informações legítimas e que são relevantes ao prosseguimento da tarefa investigatória, no sentido de se dar continuidade à tentativa de identificação dos mandantes. Tais providências investigatórias empreendidas pelo Ministério Público do Estado do Rio de Janeiro, por si só, revelam o comprometimento do Estado do Rio de Janeiro em garantir a plena execução de uma vertente investigatória no plano da quebra de sigilo telefônico, telemático e de dados, conquanto incompreensivelmente as empresas GOOGLE BRASIL INTERNET LTDA., GOOGLE LLC e o FACEBOOK que controlam os dados de milhões de cidadãos de todo o mundo, sabem o que compram, do que gostam e não gostam, o que leem, aonde vão de férias, quanto ganham, as suas lembranças fotográficas, bem como se estão buscando um carro novo ou tênis para comprar e, ainda, que são capazes de conectar e vender todas essas informações, mas INEXPLICAVELMENTE, se negam a fornecer os dados requeridos pelo Ministério Público do Estado do Rio de Janeiro e deferidas judicialmente [...]

Além disso, a própria atuação do Ministério Público do Estado do Rio de Janeiro, a quem deferi o pedido de vista em outro recurso referente ao mesmo caso, permitindo-lhe, ainda, figurar como parte interessada no âmbito desta Corte, denota

a existência de interesse no prosseguimento das medidas deferidas pelo Juízo de origem. Superada, portanto, essa alegação preliminar, *passo ao exame do mérito da* quaestio iuris.

III. POSSIBILIDADE DE QUEBRA DO SIGILO DE DADOS (REGISTROS) ESTÁTICOS: INEXISTÊNCIA DE VIOLAÇÃO DO DEVIDO PROCESSO LEGAL, DO PRINCÍPIO DA PRESUNÇÃO DE INOCÊNCIA, DA PRIVACIDADE, DO DIREITO DE ACESSO À INFORMAÇÃO E DA LIBERDADE DE COMUNICAÇÃO

A *Declaração Universal dos Direitos do Homem*, em seu art. 12, prevê que "ninguém deverá ser submetido a interferências arbitrárias na sua vida privada, família, domicílio ou correspondência, nem a ataques à sua honra e reputação" e destaca, ainda, que "contra tais intromissões ou ataques todas as pessoas têm o direito à proteção da lei". Segundo o *Alto Comissariado da ONU para Direitos Humanos:*

> [...] a privacidade é um valor em si, essencial para o desenvolvimento da personalidade e para proteção da dignidade humana, um dos principais temas da DUDH. Permite nossa proteção contra interferências não autorizadas em nossas vidas e de determinar como queremos interagir com o mundo. A privacidade nos ajuda a estabelecer fronteiras para limitar quem trem acesso aos nossos corpos, lugares e coisas, assim como nossas comunicações (Visto em: <nacoesunidas.org/artigo-12-direito-a-privacidade/>. Acesso em: 17 ago. 2020).

No mesmo sentido, a *Convenção Europeia para a Proteção dos Direitos Humanos e das Liberdades Fundamentais:*

> Art. 8º - Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência. Não pode haver ingerência de autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e construir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e a prevenção das infrações penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

A seu turno, a *Carta de Direitos Fundamentais da União Europeia*, de 2009, com a entrada em vigor do Tratado de Lisboa, em seu art. 8º, assinala:

> Art. 8º Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito. Esses dados devem ser objeto de um tratamento legal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.

E, ainda, a *Convenção Americana sobre Direitos Humanos* estabelece, em seu art. 11, § 2º, que "*[n]inguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada*, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação". No caso Vereda La Esperanza *vs*. Colômbia, a Corte Interamericana de Direitos Humanos "considerou que o âmbito da privacidade se caracteriza por ser isento e imune a invasões ou agressões abusivas ou arbitrárias por parte de terceiros ou da autoridade pública" (Disponível em: <http://www.stf.jus.br/arquivo/cms/jurisprudenciaInternacional/anexo/ConvenoAmericanasobreDireitosHumanos10.9.2018.pdf>. Acesso: em 17 ago. 2020).

Os direitos à vida privada e à intimidade fazem parte do núcleo de direitos relacionado às liberdades individuais, sendo, portanto, protegidos em diversos países e em praticamente todos os documentos importantes de tutela dos direitos humanos. Eles "salvaguardam a esfera de reserva do ser humano, insuscetível de intromissões externas (aquilo que os italianos chamam de *rizervatezza* e os americanos de *privacy*)" (BULOS, Uadi Lammêgo. *Curso de direito Constitucional*. São Paulo: Saraiva, 2009, p. 462).

No Brasil, a Constituição Federal, no art. 5º, X, estabelece: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação". *A ideia de sigilo se fundamenta diretamente nessa garantia, faceta esta que manifesta, de forma expressiva, verdadeiro direito da personalidade*, notadamente porque se traduz em uma garantia constitucional de inviolabilidade dos dados e informações inerentes a pessoa, advindas também de suas relações no âmbito digital. Como reconhece T. M. Vieira, "o exercício da privacidade nada mais representa que o exercício do Direito à liberdade de se expor ou não quanto a decidir em que medida pretende o titular revelar sua intimidade e sua vida privada para o mundo exterior" (*O direito à privacidade na sociedade da informação, efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Porto Alegre: Sérgio Antônio Fabris Editor, 2007, p. 21-22).

Em uma sociedade onde a informação é compartilhada cada vez com maior velocidade, nada mais natural que a preocupação do indivíduo em assegurar que fatos inerentes a sua vida pessoal sejam protegidos, sobretudo diante do desvirtuamento ou abuso de interesses de terceiros. Entretanto, mesmo reconhecendo que o sigilo é expressão de um direito fundamental de alta relevância ligado à personalidade, a doutrina e a jurisprudência compreendem que *não se trata de um direito absoluto*, admitindo-se a sua restrição quando imprescindível ao interesse público.

Em outras palavras, é possível mitigar o direito ao sigilo sempre que houver a necessidade de se harmonizar possível violação de outros direitos fundamentais ou de interesses constitucionalmente protegidos, notadamente diante da prática de crimes. A Carta Magna "atribuiu a tais direitos um elevado grau de proteção, de tal sorte que uma restrição apenas se justifica quando necessária a assegurar a proteção de outros direitos fundamentais ou bens constitucionais relevantes (no caso, portanto, de uma restrição implicitamente autorizada pela Constituição Federal), de modo que é em geral na esfera dos conflitos com outros direitos que se pode, em cada caso, avaliar a legitimidade constitucional da restrição" (SARLET, Ingo Wollgang *et al*. *Curso de direito constitucional*. São Paulo: Saraiva, 2016, p. 447).

De acordo com a jurisprudência do STF, "os direitos e garantias individuais não tem caráter absoluto. Não há, no sistema constitucional brasileiro, direitos ou garantias que se revistam de caráter absoluto, mesmo porque razões de relevante interesse público ou exigências derivadas do princípio de convivência das liberdades legitimam, ainda que excepcionalmente, a adoção, por parte dos órgãos estatais, de medidas restritivas das prerrogativas individuais ou coletivas, desde que respeitados os termos estabelecidos pela própria Constituição" (*MS nº 23.452/RJ*, Rel. Ministro *Celso de Mello*, DJ 15/5/2000).

De fato, embora deva ser preservado na sua essência, este Superior Tribunal de Justiça, na linha da orientação firmada pela Suprema Corte, entende que é possível afastar a sua proteção *quando presentes circunstâncias que denotem a existência de interesse público relevante, invariavelmente por meio de decisão proferida por autoridade judicial competente, suficientemente fundamentada, na qual se justifique a necessidade da medida para fins de investigação criminal ou de instrução processual criminal*, sempre lastreada em indícios que devem ser, em tese, suficientes à configuração de suposta ocorrência de crime sujeito à ação penal pública.

Não descuro, na linha das diretrizes traçadas pelo entendimento predominante, em casos mais comuns, onde se pleiteia a *interceptação de dados informáticos*, seja necessário estarem presentes reais indícios que apontem a prática de uma infração penal pelo titular das informações sigilosas afetadas pela decisão, sobretudo porque o fato indiciário, que autoriza um juízo de probabilidade, não se identifica com a mera suspeita ou com simples conjectura desacompanhada de elementos fáticos concretos. Na hipótese, verifica-se que a investigação levada a cabo na origem procura desvendar a prática de três homicídios, dois deles consumados. Todavia, a ordem judicial de coleta de registros de dados se dirige a um número indeterminado de pessoas, como objetado pelas recorrentes.

No particular, afirmam que a ordem jurídica interna dispõe, de forma específica, taxativa e excepcional, sobre as hipóteses em que se admite quebra de sigilo e fornecimento de dados. Nos termos do art. 22 da Lei nº 9.296/96, da Resolução CNJ nº 59/2008, do art. 22 do Marco Civil da Internet e do art. 11 do Decreto Federal nº 8.771/2016, inexiste autorização legal para a determinação da quebra de sigilo de um conjunto não identificado de pessoas, unidas tão somente pela circunstância

aleatória de terem transitado, em certo lapso de tempo, por *diversas coordenadas geográficas do Município do Rio de Janeiro/RJ (Ofício nº 4041/2018 e Ofício nº 4047/2018*, sem qualquer imputação de conduta ilícita aos afetados.

Afirmam que o critério determinado pela autoridade coatora "criam risco concreto de se afetar um número muito elevado de pessoas inocentes, já que abrangem extensas áreas do Rio de Janeiro – os polígonos englobam residências, repartições públicas, cartórios, escritórios de advocacia, hospitais, sindicatos, bancos, igrejas, escolas, hotéis, lojas, avenidas e pontos turísticos – parte considerável deles sequer diz respeito à data e local do crime" (fl. 154).

Defendem que a quebra do sigilo de dados tem que obrigatoriamente indicar as pessoas suspeitas que serão investigadas e objeto da medida invasiva. Isso seria uma exigência contida no art. 5º, X, XII e 93, IX, ambos da Constituição Federal, os quais seriam regulamentados pelo art. 2º. da Lei nº 9.296/96, pela Resolução CNJ nº 59/2008, pelo art. 22 do Marco Civil da Internet (Lei nº 12.965/14) e pelo art. 11 do Decreto-Federal nº 8.771/2016. Aduziram, no particular, que não existe previsão no ordenamento jurídico brasileiro para fornecimento indiscriminado de dados de um sem-número de pessoas que simplesmente buscaram por informações na internet em determinado.

Feitas essas considerações, é necessário, para perfeita compreensão do caso vertente, em primeiro lugar, avaliar a extensão da decisão proferida pelo Magistrado de primeiro grau e impugnada neste recurso, o qual se insurge *especificamente em relação à seguinte determinação* (fls. 56-60):

> a) Que o provedor de aplicação de internet GOOGLE INC., sob pena de incursão no crime de desobediência, além de multa diária no valor de R$100.000,00 (cem mil reais), até o limite de R$ 3.000.000,00 (três milhões de reais), em caso do descumprimento de determinação judicial, ou de seu cumprimento parcial, nos termos do art. 537 do NCPC, forneça e disponibilize à Autoridade Policial e ao Ministério Público, no prazo de 05 (cinco) dias, a contar do recebimento desta ordem, e usando-se de *parâmetro os polígonos e conjuntos formados e relacionados a seguir* [...] *na busca do levantamento destes usuários através das contas vinculadas aos dispositivos identificados e operando na área delimitada de cada conjunto de polígonos* com sistemas operacionais IOS, WINDOWS MOBILE, sistema de gerenciamento GOOGLE/ANDROID, pelo aplicativo GOOGLE MAPS ou pelo aplicativo WAZE [...].

Observe-se que a determinação judicial *se referiu a dados estáticos (registros), relacionados à identificação de usuários que operaram em determinada área delimitada*. Tal situação, que configura quebra de sigilo de dados (registros) informáticos, é

de suma importância, *porque se distingue das interceptações das comunicações*. Nas palavras de Gustavo Badaró, "a tutela constitucional da liberdade das comunicações telefônicas (art. 5º, XII) não inclui os dados de registro das ligações telefônicas (p. ex: número da linha telefônica para a qual foi feita a ligação pelo telefone interceptado ou número da linha telefônica que efetuou ligação para linha interceptada, horário das ligações etc.) que ficam armazenados nas operadoras dos serviços de telefonia, e permanecem protegidos pela garantia geral da intimidade e da vida privada (CR, art. 5º, X)" (*Processo penal*. Rio de Janeiro: Campos; Elsevier, 20112, p. 348).

Com efeito, pela determinação do Magistrado de primeiro grau, verifica-se que *houve a ordem de quebra de dados informáticos estáticos*, os quais se referem à identificação de usuários de aplicativos em determinado perímetro geográfico, diversamente do que ocorre com as interceptações das comunicações, as quais dão acesso ao fluxo de comunicações de dados, isto é, ao conhecimento do conteúdo da comunicação travada com o destinatário dela.

Há uma distinção conceitual entre a quebra de sigilo de dados armazenados e a interceptação do fluxo de comunicações. Segundo o entendimento do STF, *mutatis mutandis*, "*[n]ão se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional é da comunicação de dados e não dos dados*" (*HC nº 91.867/PA*, Rel. Ministro *Gilmar Mendes*, DJe 20/9/2012, destaquei).

Decerto que o art. 5º, X, da CF/88, garante a inviolabilidade da intimidade e da privacidade, inclusive quando os dados informáticos constarem de banco de dados ou de arquivos virtuais mais sensíveis. Entretanto, repita-se, o acesso a esses dados registrados ou arquivos virtuais não se confunde com a interceptação das comunicações e, por isso mesmo, a amplitude de proteção não pode ser a mesma.

A propósito, já decidiu o STF que "a proteção contida no artigo 5º, inciso XII, da Constituição Federal *restringe-se ao sigilo das comunicações telefônicas e telemáticas, não abrangendo os dados já armazenados em dispositivos eletrônicos*" (*HC nº 167.720/SP*, Rel. Ministro *Luiz Fux*, DJe 14/4/2019, grifei). Logo, o ordenamento jurídico brasileiro tutela de maneira diferente o *conteúdo das comunicações* mantidas entre indivíduos e, a seu turno, as *informações de conexão e de acesso a aplicações de internet,* garantindo proteção também a essa segunda categoria de dados, ainda que em dimensão não tão ampla.

Sob tal perspectiva, os dispositivos que se referem às interceptações das comunicações indicados pelos recorrentes não se amoldam ao caso *sub examine*. O procedimento de que trata o art. 2º da Lei nº 9.296/1996, cujas rotinas estão previstas na Resolução nº 59/2008 (com alterações ocorridas em 2016) do CNJ, os quais regulamentam art. 5º, XII, da CF, *não se aplica a procedimento que visa obter dados estáticos armazenados em seus servidores e sistemas informatizados de um provedor de serviços de internet*. A quebra do sigilo de dados, na hipótese, corresponde à obtenção de registros informáticos existentes ou dados já coletados.

Não há como pretender dar interpretação extensiva aos referidos dispositivos, de modo a abranger a requisição feita em primeiro grau, porque a ordem é dirigida a um provedor de serviço de conexão ou aplicações de internet, cuja relação é *devidamente prevista no Marco Civil da Internet, o qual não prevê, entre os requisitos que estabelece para a quebra do sigilo, que a ordem judicial especifique previamente as pessoas objeto da investigação ou que a prova da infração (ou da autoria) possa ser realizada por outros meios*.

No particular, os arts. 22 e 23 do Marco Civil da Internet estabelecem o seguinte:

> Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o *fornecimento de registros de conexão ou de registros de acesso a aplicações de internet*.
>
> Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:
>
> *I - fundados indícios da ocorrência do ilícito;*
>
> *II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e*
>
> *III - período ao qual se referem os registros.*
>
> Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

Como se observa, os referido dispositivos, que tratam especificamente do procedimento de que cuidam os autos, *não exigem a indicação ou qualquer elemento de individualização pessoal na decisão judicial. Tal exigência, por certo, revelar-se-ia verdadeiro contrassenso, na medida em que o objetivo da lei é possibilitar essa identificação.*

Além disso, o art. 10, parágrafo único, do mesmo diploma, por sua vez, prevê:

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
>
> § 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma

> autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º .
>
> § 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

Há, como se verifica, menção aos registros de conexão e de acesso a aplicações, associados ou não a outros dados pessoais coletados pelos provedores, que podem ser objeto de requisição judicial para identificação dos usuários desses serviços. *O objetivo precípuo da previsão legal é possibilitar a identificação do usuário do serviço ou terminal, isto é, possibilitar a descoberta de quem fez uso do serviço ou acessou um determinado terminal, em algum momento e em certa localidade.*

Importante salientar que os registros que serão coletados, além de não servirem para quaisquer outras finalidades que não a elucidação dos graves delitos, *devem ser submetidos ao filtro investigativo, que deve descartar qualquer informação que não tenha relevância ou relação com o objetivo da investigação*. Vale dizer, os registros de pessoas não envolvidas com os fatos objeto de investigação continuarão protegidos pelo sigilo, sem a identificação dos titulares que possa vir a ser dada publicidade.

Assim, devem ser afastadas as alegações das insurgentes de que a quebra de sigilo poderá acarretar dano objetivo irreversível à privacidade de um sem-número de cidadãos inocentes (fl. 151). *A determinação judicial envolve a obtenção de registros que apenas identificam os usuários*. Certamente que, após uma filtragem investigativa, haverá a seleção daqueles casos que possam, em um juízo de probabilidade, ser objeto de medida mais invasiva a ser requisitada e apreciada pelo judiciário.

Assinalo, ainda, que todo e qualquer tipo de dado coletado por provedores de serviços na Internet podem ser utilizados para fins de investigação penal ou de instrução criminal. Não somente registros de conexão (*logs*) à rede e aplicações, mas todos os dados de natureza pessoal ou não, que decorram de qualquer operação de coleta, guarda ou tratamento realizada por provedores de conexão e aplicações de internet, podem ser requisitados pelas autoridades judiciais para possibilitar a investigação de ilícitos e facilitar a atividade de persecução penal.

Aliás, *os provedores inclusive têm a obrigação de manter os dados armazenados em seus servidores, conforme assinala o art. 15 do Decreto nº 8.771/2016, "em formato interoperável e estruturado, para facilitar o acesso decorrente de decisão judicial ou determinação legal"*.

III. 1. INAPLICABILIDADE DOS PRECEDENTES INDICADOS NO RECURSO E NO PARECER JURÍDICO APRESENTADO PARA A HIPÓTESE DOS AUTOS

Feitas as considerações acerca da distinção existente entre o que vem a ser o sigilo das comunicações e o sigilo dos dados informacionais já armazenados pelo provedor, impõe breve análise sobre os precedentes citados nas razões do recurso e, também, no parecer jurídico juntado aos autos, os quais, na visão das recorrentes, se aplicariam ao caso em exame e justificariam o pedido formulado na inicial.

De início, apenas para facilitar a melhor compreensão dos argumentos que serão expostos, distingo os julgados apresentados no recurso em três situações: *1ª) os proferidos em liminar ou em tutela provisória; 2º) os proferidos em casos de interceptações de comunicações; e, por fim, 3º) os proferidos com base em situações absolutamente distintas da argumentada nesta ocasião.*

Em relação à primeira situação, sobressaem, exemplificativamente, a *liminar deferida* no *RMS nº 59.716/RS*, de relatoria do Ministro *Sebastião Reis*, publicado no DJe 19/12/2018 e a *Tutela Provisória nº 292*, de relatoria do Ministro *Antônio Saldanha Palheiro*, publicada no Dje 6/9/2017. Em ambos os casos, o exame do tema, que é similar ao debatido nesta oportunidade, circunscreveu-se a subsidiar mero juízo de verossimilhança. Vale dizer, *não houve o enfrentamento do tema pelo colegiado, com o julgamento de mérito dos recursos interpostos*. A relevância e a complexidade do tema até justificariam a concessão de pedido de urgência, como explicitado nos casos referidos, mas isso não significa que o pensamento externado *initio litis* corresponda à orientação que será fixada com o julgamento de mérito.

No que tange à segunda situação, é indicado, entre outros, o *RHC nº 99.735/SC*, de relatoria da Ministra *Laurita Vaz*, publicado no DJe 12/12/2018, que *trata de interceptação telefônica e de espelhamento de conversas travadas no Whatsapp*. Não há, portanto, similaridade com a hipótese dos autos, a qual *não trata de interceptação de comunicações, mas de acesso a dados estáticos já armazenados de identificação*.

Por fim, quanto à terceira situação, cito os precedentes proferidos no *HC nº 137.349/SP*, de relatoria da Ministra *Maria Thereza*, publicado no DJe 30/5/2011 e o *AgRg no HC nº 435.934/RJ*, de relatoria do Ministro *Sebastião Reis Júnior*, publicado no DJe 19/11/2019, ambos do STJ. No STF, o proferido no *HC nº 84758/GO*, de relatoria do Ministro *Celso de Mello*, publicado no DJ 16/6/2006.

No *HC nº 137.349/SP*, a discussão se cingiu à possibilidade de *denúncia anônima subsidiar a quebra de sigilo de dados*, sem que houvesse investigação preliminar. Já o *AgRg no HC nº 435.934/RJ* tratava da possibilidade de *busca e apreensão domiciliar* sem a necessária individualização. E, por último, o *HC nº 84.758/GO*, da relatoria do Ministro *Celso de Mello*, examinou a possibilidade da *quebra de sigilo bancário*.

Como se observa, as três situações, que foram resumidas a partir de precedentes indicados pelas insurgentes com a finalidade de reforçar a argumentação feita no recurso, *ou tratam de decisão precária proferida em liminar e em tutela provisória, ou de questões que não se coadunam com a situação dos autos pela absoluta falta de similaridade de casos*.

IV. FUNDAMENTAÇÃO ADEQUADA DA DECISÃO QUE DETERMINOU A QUEBRA DO SIGILO E FORNECIMENTO DOS REGISTROS

Conforme dispõe o art. 93, IX, da CF, "todos os julgamentos dos órgãos do Poder Judiciário serão públicos, e fundamentadas todas as decisões, sob pena de nulidade, podendo a lei limitar a presença, em determinados atos, às próprias partes e a seus advogados, ou somente a estes, em casos nos quais a preservação do direito à intimidade do interessado no sigilo não prejudique o interesse público à informação".

Com supedâneo nessas premissas e no fato de que a decisão judicial, em caso como o dos autos, deve descrever os indícios da ocorrência do ilícito, a justificativa da utilidade da requisição e o período ao qual se referem os registros extraem-se da decisão impugnada, no que interessa, as seguintes passagens (fls. 56-60):

> Trata-se de procedimento instaurado para apurar a autoria e a materialidade dos crimes de homicídio qualificado cometidos em face de Marielle Francisco da Silva e Anderson Pedro Matias Gomes e de homicídio qualificado tentado em face de Fernanda Gonçalves Chaves, ocorridos no dia 14/03/2018, por volta das 21h, na Rua Joaquim Palhares, em frente ao número 330, no Bairro do Estácio, nesta cidade.
>
> Conforme as investigações policiais, há informações nos autos deste inquérito no sentido de que as vítimas foram atingidas por disparos de arma de fogo supostamente realizados por ocupantes de um veículo Chevrolet/Cobalt, cor prata. Durante realização da perícia técnica foram arrecadados, próximo ao carro que transportava as vítimas, vários componentes de munição, a saber, estojos de calibre 9 mm, pertencentes ao lote UZZ18, vendido à Polícia Federal. Após a colheita de depoimentos de amigos e familiares das vítimas, não foi possível delinear a suposta autoria delitiva.
>
> A autoridade policial, às fls. 954/1002 do apenso sigiloso V, representou pela decretação da QUEBRA DE SIGILO DE DADOS DE COMUNICAÇÕES TELEFÔNICAS, bem como, pela QUEBRA DE SIGILO DE DADOS BANCÁRIOS.
>
> O Ministério Público às fls. 1008/1025 opinou pelo deferimento da representação da Autoridade Policial, com algumas modificações.
>
> Compulsando os autos, tenho que se encontram íntegros os motivos a ensejarem o deferimento dos pedidos ora apresentado, eis que imprescindíveis para a linha de investigação adotada, bem como pelo fato de que não há outro meio viável a permitir o avanço da instrução criminal.

> Assim, conclui-se que as medidas ora pleiteadas são providências que se impõem, pois indispensáveis para se chegar a todos aqueles que, de alguma forma, possam ter participação nos crimes que se apuram, bem como das circunstâncias em que se desenvolveram os fatos criminosos. As medidas são juridicamente viáveis, contando com expressa permissão constitucional (art. 5°, inciso XII da Constituição, art. 2°, incisos I a III da Lei nº 9296/96, art. 22 da Lei nº 12965/14, ART. 1° §4° inciso IX da lei complementar 105). Não há direito absoluto e os direitos à privacidade em jogo cedem diante da necessidade de apuração dos crimes, conforme ponderação já realizada pelo Constituinte e pelo legislador complementar e ordinário.
>
> [...]
>
> Assim, determino:
>
> a) Que o provedor de aplicação de internet GOOGLE INC., sob pena de incursão no crime de desobediência, além de multa diária no valor de R$100.000,00 (cem mil reais), até o limite de R$ 3.000.000,00 (três milhões de reais), em caso do descumprimento de determinação judicial, ou de seu cumprimento parcial, nos termos do art. 537 do NCPC, forneça e disponibilize à Autoridade Policial e ao Ministério Público, no prazo de 05 (cinco) dias, a contar do recebimento desta ordem, e usando-se de *parâmetro os polígonos e conjuntos formados e relacionados a seguir* [...]
>
> *na busca do levantamento destes usuários através das contas vinculadas aos dispositivos identificados e operando na área delimitada de cada conjunto de polígonos* com sistemas operacionais IOS, WINDOWS MOBILE, sistema de gerenciamento GOOGLE/ANDROID, pelo aplicativo GOOGLE MAPS ou pelo aplicativo WAZE [...].

Como se nota, *tanto os indícios da prática do crime, como a justificativa para a utilização da medida e o período ao qual se referem os registros foram devidamente expostos* pelo Magistrado de primeiro grau. Realço que a natureza da medida não se coaduna com a imposição de prévia indicação dos autores da infração penal objeto de investigação, porquanto é precisamente esse o objetivo da medida, ou seja, descobrir, por meio da requisição de registros e dados, eventual autor ou partícipe do delito.

V. PROPORCIONALIDADE

É de uso recorrente a doutrina que propõe a *técnica da ponderação* de interesses, ante o *princípio da proporcionalidade***,** como mecanismo de solução para a colisão entre direitos fundamentais estruturados como princípios. Muito simplificativamente,

a técnica, desenvolvida por Roberto Alexy, consiste em realizar o sopesamento entre os princípios incidentes no caso concreto, de modo a indicar qual terá maior peso e, portanto, precedência no deslinde da questão.

E nessa aferição da proporcionalidade da medida que, de algum modo, esteja a afetar um direito fundamental, há de se observar que o princípio em exame se apresenta sob três perspectivas, derivações ou subprincípios: a) *adequação ou idoneidade* (dos meios empregados para se atingir o resultado); b) *necessidade ou proibição de excesso* (para avaliar a existência ou não de outra solução menos gravosa ao direito fundamental em foco); c) *proporcionalidade em sentido estrito* (para aferir a proporcionalidade dos meios empregados para o atingimento dos fins almejados).

O próprio Supremo Tribunal Federal reconhece a técnica da ponderação como instrumento de solução de conflitos de interesses embasados em proteção de nível constitucional. Ilustrativamente,

> [e]m síntese, a aplicação do princípio da proporcionalidade se dá quando verificada restrição a determinado direito fundamental ou um conflito entre distintos princípios constitucionais de modo a exigir que se estabeleça o peso relativo de cada um dos direitos por meio da aplicação das máximas que integram o mencionado princípio da proporcionalidade. (*Intervenção Federal nº 2.257-6/SP*, Rel. Ministro *Gilmar Mendes*, Pleno).

Dito isso, a colisão entre o direito coletivo à segurança (e, consequentemente, direito à apuração e à punição de quem tenha violado a lei penal), e outros direitos fundamentais constitucionalmente assegurados deve partir da percepção de que:

> A segurança é um bem protegido pela Constituição Federal de 1988 e constitui, também, um direito fundamental da pessoa. Situada no mesmo nível dos demais direitos fundamentais, se em conflito com outros direitos fundamentais, *a segurança é um direito que pode ser levado à balança da ponderação*. O seu "peso", avaliado no caso concreto, poderá, dependendo das circunstâncias, *fazê-la preponderar sobre outros direitos ou bens constitucionalmente protegidos*. (PRADO, Fabiana Lemes Zamalloa do. *A ponderação de interesses em matéria de prova no processo penal.* São Paulo: IBCCRIM, 2006, p. 196-197).

Trazendo essa doutrina para o exame do caso concreto – em que o direito à segurança pública e à preservação e restauração da ordem pública tem algum resvalo no direito ao sigilo de dados –, nota-se a realização da proporcionalidade em suas três diretrizes essenciais. Ela é *adequada,* na medida em que serve como meio auxiliar

na elucidação dos delitos, cuja investigação se arrasta por dois anos, sem que haja uma conclusão definitiva. É *necessária*, diante da gravidade e complexidade do caso e da inexistência de outros meios menos gravosos para se alcançar os legítimos fins investigativos. E, por fim, é *proporcional em sentido estrito*, porque a restrição aos direitos fundamentais que dela redundam não ensejam gravame as pessoas afetadas, as quais não terão seu sigilo de dados registrais publicizados, certo, ainda, se não constatada sua conexão com o fato investigado, serão descartados.

Importa enfatizar que se pretende, com a medida contestada pela recorrente, a apuração de gravíssimos crimes contra a vida de quem morreu por sua defesa de direitos humanos, rotineiramente violados por terceiros e por agentes do Estado. Sem embargo, como assinalei em voto proferido nos autos do IDC nº 24, esse assassinato, ao que se pode inferir da narrativa sobre o fato, *foi cometido em razão não apenas da atividade da parlamentar Marielle Franco, em defesa dos direitos humanos. Tudo indica tenha sido também motivado porque essa pauta era conduzida por uma mulher, vinda da periferia, negra e lésbica, ingredientes que, em uma cultura patriarcal, misógina, racista e preconceituosa*, potencializaram a reação de quem se sentia incomodado, quer pelas denúncias feitas no exercício do mandato parlamentar da vereadora Marielle Franco, quer pela postura de uma mulher intimorata, que, representando as citadas minorias, arrostou milicianos e policiais envolvidos na reiterada e permanente violação dos direitos das pessoas que habitam as comunidades do Rio de Janeiro.

Aliás, nos autos do referido Incidente de Deslocamento de Competência, relatado pela em. Ministra Laurita Vaz, consta manifestação do Ministério Público Federal, em que aponta o quadro de elevada violência urbana no Estado do Rio de Janeiro, que motivou, inclusive, a intervenção federal na segurança pública. E, em alusão ao Inquérito da Polícia Federal que investigou a atuação da Polícia Civil no caso Marielle, afirmou o *Parquet* Federal que:

> [...]
>
> Em 15 de março de 2019, dez relatores e especialistas da Organização das Nações Unidas e da Comissão Interamericana de Direitos Humanos (CIDH) manifestaram-se, em comunicado, que o "Brasil deve garantir que os assassinos da defensora de direitos humanos e vereadora Marielle Franco sejam levados à justiça".
>
> Em 08 de outubro de 2019, documento de pesquisa da Anistia Internacional, lançado no relatório "Lutando pelo fim da violência contra mulheres na política", em Nova York, cobrou providências das autoridades brasileiras no caso Marielle Franco.
>
> E o tempo corre a favor da impunidade e contra a eficiência na investigação. Com efeito, de acordo Conselho Nacional do Ministério Público, as taxas de elucidação de homicídios no Brasil não ultrapassam 8%. Em países como o Reino Unido e a França,

> esses índices chegam a 90% e 80%, respectivamente. E mais: 78% dos inquéritos de homicídio são arquivados principalmente pelo longo tempo entre a data e os trabalhos de investigação.
>
> Tal realidade, no caso concreto, agrava-se. O tempo está passando, não se sabe dos mandantes e é possível que a investigação esteja, ainda que parcialmente, sob a influência de fato, ainda que remota, de envolvidos com o "ESCRITÓRIO DO CRIME".
>
> [...]
>
> Preenchido este requisito, também se encontra presente a grave violação de direitos humanos. Como narrado na inicial, o assassinato d**e** Marielle Franco consistiu em feminicídio de importante e *ascendente defensora de direitos humanos,* que havia sido, ademais, eleita vereadora (quinta maior votação) na cidade do Rio de Janeiro, por partido de oposição (Partido Socialismo e Liberdade – PSOL), *adotando pautas de promoção de direitos de afrodescendentes, em prol das mulheres e no combate à violência policial e aos grupos paramilitares de atuação notória no Rio de Janeiro, denominados de "milicianos", que são compostos por policiais ou ex-policiais, contando, para seu agir desenvolto, com laços com o aparato oficial.*
>
> Essas características da vítima geram importante efeito inibidor para o exercício dos direitos humanos na sociedade, *pois os assassinos demonstram sua força e certeza de impunidade ao atingir um defensor ou defensora de direitos humanos, intimidando e deixando inseguros os demais membros do grupo vulnerável envolvido***.**

Efetivamente, quando do julgamento do caso *Ximenes Lopes vs*. *Brasil*, (sentença de 4 de julho de 2006), a Corte Interamericana de Direitos Humanos, como já asseriu em diversos outros casos, pontuou que "a obrigação do Estado de 'garantir' o direito humano à vida implica prevenir violações a tal direito, *investigar as violações ao direito à vida, punir os responsáveis*, e reparar aos familiares da vítima, quando os responsáveis tenham sido agentes do Estado".

Nesse contexto, concluiu: "*O Estado não somente incorre em responsabilidade internacional por violação ao direito à vida* quando seus agentes privam alguém de tal direito, mas também *quando, apesar de não ter violado diretamente tal direito, não adota as medidas de prevenção necessária e/ou não efetua uma investigação séria*, por um órgão independente, autônomo e imparcial, de privações do direito à vida cometida seja por seus agentes ou por particulares".

Assim, a ordem judicial para quebra do sigilo dos registros, delimitada por parâmetros de pesquisa em determinada região e por período de tempo, não se mostra medida desproporcional, *porquanto, tendo como norte a apuração de gravíssimos crimes*

cometidos por agentes públicos contra as vidas de três pessoas – mormente a de quem era alvo da emboscada, pessoa dedicada, em sua atividade parlamentar, à defesa dos direitos de minorias que sofrem com a ação desse segmento podre da estrutura estatal fluminense –, não impõe risco desmedido à privacidade e à intimidade dos usuários possivelmente atingidos pela diligência questionada**.** A existência dessa delimitação por *parâmetros e por lapso de tempo* serve inclusive como limitador do alcance da medida.

A finalidade de elucidação dos crimes, de alta complexidade investigativa, justifica a requisição de dados, cuja ciência pelas autoridades que atuam no caso, não causará reflexos significativos nos direitos fundamentais das pessoas abrangidas pela determinação, como exposto alhures.

VI. DISPOSITIVO

À vista do exposto, *nego provimento ao recurso em mandado de segurança*.

RECURSO EM MANDADO DE SEGURANÇA Nº 61.302 / RIO DE JANEIRO (2019/0199132-0)

VOTO

O EXMO. SR. MINISTRO SEBASTIÃO REIS JÚNIOR: Sr. Presidente, serei breve, considerando que a maioria já se encontra formada.

Peço vênia para divergir do eminente Relator e da maioria já firmada por entender que não vejo como prevalecer a decisão que determinou à recorrente a identificação dos IPs ou Device IDs que tenham se utilizado do Google Maps e/ou plataformas Waze no período compreendido entre 10/3/2018 a 14/3/2018, para realizar consulta do seguinte endereço de destino: Rua dos Inválidos, 122, ou Rua dos Inválidos, bem como os mesmos dados referentes a quem tenha se utilizado do Google Busca no período compreendido entre os mesmos dias, para realizar consultas dos seguintes parâmetros de pesquisa: Mariele Franco; Vereadora Mariele Franco; Agenda Vereadora Mariele; Casa das Pretas; Rua dos Inválidos, 122; ou Rua dos Inválidos.

Primeiro, esclareço que, no meu entender, em que pese em um primeiro momento não haver a identificação pessoal do usuário, é evidente que tal determinação busca, ao final, essa identificação, senão não teria razão de ser. E assim há, senão em um primeiro momento, invasão à privacidade dos usuários porque tais dados vão permitir não só saber onde eventualmente o usuário esteve em um período de 4 dias, bem como quais foram as buscas que fez na internet no mesmo período.

Segundo, esclareço que vejo possível sim a solicitação por parte da Justiça de informações como estas que estão em debate neste momento, desde que devidamente justificadas e especificadas.

Porém, levando em consideração o princípio constitucional que protege, em regra, a privacidade, bem como o disposto no art. 11, § 3º, do Decreto nº 8.771/16, que

expressamente veda pedidos genéricos, entendo que a amplitude do que foi determinado torna a decisão questionada ilegal. E isso porque a decisão não apresenta, em qualquer momento, justificativa suficiente quanto à extensão das informações solicitadas.

A determinação judicial cuida de um período de quatro dias (por que não três ou cinco, ou seis, ou dez?) e atinge um número não identificado de pessoas sem qualquer justificativa para tanto.

Assim, seguindo, inclusive, o que foi exposto pelo douto voto vencido na origem, bem como na manifestação do próprio Ministério Público nestes autos, entendo que a segurança há de ser concedida como requerida.

É como voto.

CERTIDÃO DE JULGAMENTO
TERCEIRA SEÇÃO

Número Registro: 2019/0199132-0

PROCESSO ELETRÔNICO

RMS 61.302 / RJ

MATÉRIA CRIMINAL

Números Origem: 0016639-30.2019.8.19.0000 00166393020198190000 00720266120188190001 00729689620188190000 166393020198190000 3062439177732

PAUTA: 26/08/2020

JULGADO: 26/08/2020

SEGREDO DE JUSTIÇA

Relator

Exmo. Sr. Ministro ROGERIO SCHIETTI CRUZ

Presidente da Sessão

Exmo. Sr. Ministro NEFI CORDEIRO

Subprocuradora-Geral da República

Exma. Sra. Dra. JULIETA E. FAJARDO C. DE ALBUQUERQUE

Secretário

Bel. GILBERTO FERREIRA COSTA

AUTUAÇÃO

RECORRENTE: GOOGLE BRASIL INTERNET LTDA.
RECORRENTE: GOOGLE LLC
ADVOGADOS: EDUARDO BASTOS FURTADO DE MENDONÇA - RJ130532
FELIPE MENDONÇA TERRA - RJ179757
NAIANA DO AMARAL PORTO - RJ167818
JACQUELINE DE SOUZA ABREU - SP356941
RECORRIDO: MINISTÉRIO PÚBLICO DO ESTADO DO RIO DE JANEIRO
INTERES.: FACEBOOK SERVIÇOS ONLINE DO BRASIL LTDA.
ADVOGADOS: CARLOS ANTÔNIO PENA - SP105802
ANTÔNIO SÉRGIO ALTIERI DE MORAES PITOMBO - SP124516
GUILHERME ALFREDO DE MORAES NOSTRE - SP130665
CLAUDIO MAURO HENRIQUE DAÓLIO - SP172723
FLÁVIA MORTARI LOTFI - SP246694
IZABEL DE ARAÚJO CORTEZ - SP235560
BEATRIZ DE OLIVEIRA FERRARO - SP285552
JULIA THOMAZ SANDRONI - RJ144384
LARA MAYARA DA CRUZ - SP305340
RAFAEL SILVEIRA GARCIA - DF048029
BIANCA DIAS SARDILLI - SP299813
ASSUNTO: DIREITO PROCESSUAL PENAL

SUSTENTAÇÃO ORAL

O Dr. Eduardo Bastos Furtado de Mendonça sustentou oralmente pelas partes recorrentes: Google Brasil Internet Ltda. e Google LLC.

O Dr. Orlando Carlos Neves Belém, Procurador de Justiça, sustentou oralmente pela parte interessada: Ministério Público do Estado do Rio de Janeiro.

CERTIDÃO

Certifico que a egrégia TERCEIRA SEÇÃO, ao apreciar o processo em epígrafe na sessão realizada nesta data, proferiu a seguinte decisão:

A Terceira Seção, por maioria, negou provimento ao recurso em mandado de segurança, nos termos do voto do Sr. Ministro Relator. Vencido o Sr. Ministro Sebastião Reis Júnior que dava provimento ao recurso.

Os Srs. Ministros Reynaldo Soares da Fonseca, Ribeiro Dantas, Antonio Saldanha Palheiro, Joel Ilan Paciornik, Felix Fischer, Laurita Vaz e Jorge Mussi votaram com o Sr. Ministro Relator.

Votou vencido o Sr. Ministro Sebastião Reis Júnior.

Presidiu o julgamento o Sr. Ministro Nefi Cordeiro.